PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-332744
(43)Date of publication of application : 30.11.2000

(51)Int.CI. H04L 9/08
G09C 1/00
H04L 9/32

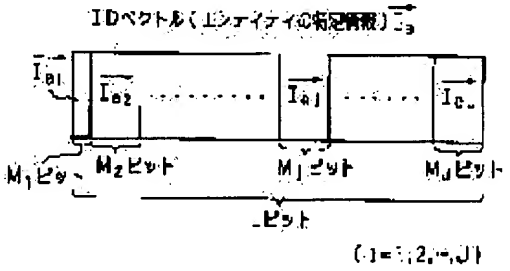
(21)Application number : 11-139285
(22)Date of filing : 19.05.1999

(71)Applicant : MURATA MACH LTD
KASAHARA MASAO
TSUJII SHIGEO

(72)Inventor : KASAHARA MASAO
MURAKAMI YASUMICHI
TSUJII SHIGEO

(54) SECRET KEY GENERATING METHOD AND CIPHERING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain higher tolerance to a coalition attack by making the value for respective components of divided vectors different, showing specific divided information obtained by dividing specific information of an entity into blocks, setting individual secret random numbers characteristic of entities set by the divided blocks, and generation a secret key by using an individual secret random number and a divided vector.
SOLUTION: ID vectors as prescribed information representing the names, addresses, etc., of respective entities are generated as L-dimensional binary vectors and divided into J ID divided vectors Iej (j=1, 2,..., J) by block size M1 bits, M2 bits,..., and MJ bits. In each ID divided vector Iej, an individual secret random number is not fixed, and mutually different individual secret random numbers are set for respective components in the ID divided vectors Iej. A set individual secret random number and an ID divided vector Iej are used to generate a secret key which is unique to each entity.



LEGAL STATUS

[Date of request for examination] 31.10.2000
[Date of sending the examiner's decision of rejection] 02.12.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11) 許出願公開番号
特開2000－332744
（P2000－332744A）
(43)公開日　平成12年11月30日(2000.11.30)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｄ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６３０	Ｇ０９Ｃ	1/00	６３０Ｅ
					６３０Ｄ
		６６０			６６０Ｆ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６０１Ｅ

審査請求　未請求　請求項の数３　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平11－139285

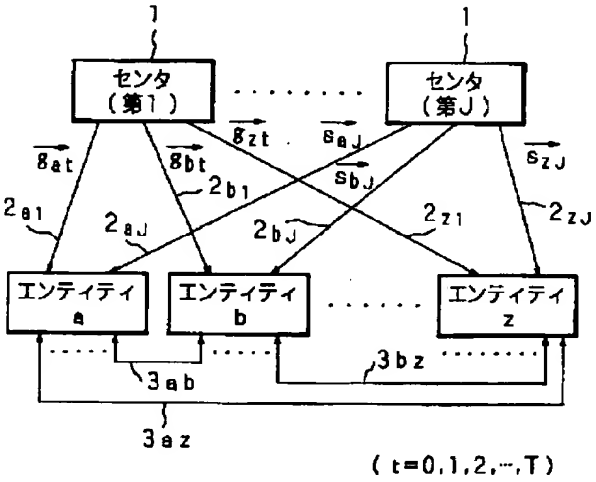
(22)出願日　平成11年５月19日(1999.5.19)

(71)出願人　000006297
村田機械株式会社
京都府京都市南区吉祥院南落合町３番地
(71)出願人　597008636
笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(71)出願人　598159964
辻井　重男
東京都渋谷区神宮前四丁目２番19号
(72)発明者　笠原　正雄
大阪府箕面市粟生外院４丁目15番３号
(74)代理人　100078868
弁理士　河野　登夫

最終頁に続く

(54)【発明の名称】　秘密鍵生成方法及び暗号化方法

(57)【要約】
【課題】　結託攻撃に対して強いＩＤ－ＮＩＫＳによる暗号通信方法を提供する。
【解決手段】　複数設けられた各センタ１は、各エンティティの特定情報（ＩＤ情報）を分割した分割ベクトルと、分割ベクトル内の各成分毎に相異ならせて設定した個人秘密乱数とを利用して、各エンティティ固有の秘密鍵を生成して配布する。各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割ベクトルに対応する成分を使用して共通鍵を生成する。各分割ベクトルを、誤り訂正符号の符号語で構成する。



1

【特許請求の範囲】

【請求項１】　エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて前記秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項２】　各エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて各エンティティ固有の秘密鍵を生成することを特徴とする暗号化方法。

【請求項３】　エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、前記分割特定情報の各ブロックを誤り訂正符号の符号語で構成することを特徴とする秘密鍵生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、エンティティ固有の秘密鍵を生成する秘密鍵生成方法、及び、情報の内容が当事者以外には判らないように情報を暗号化する暗号化方法に関する。

【０００２】

【従来の技術】高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

2

【０００４】暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。このような共通鍵暗号方式の従来例は、次のような３種の方法に分類できる。

【０００５】①　第１の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法。

②　第２の方法

暗号通信の都度、予備通信により鍵を共有し合う方法（Diffie-Hellmanによる鍵共有方式，公開鍵方式による鍵配送方式など）。

③　第３の方法

各ユーザ（エンティティ）の氏名，住所などの個人を特定する公開された特定情報（ＩＤ（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ，受信側のエンティティが独立に同一の共通鍵を生成する方法（ＫＰＳ（Key Predistribution System），ＩＤ－ＮＩＫＳ（ID-based Non-Interactive Key Sharing Schemes）など）。

【０００６】このような従来の３種の方法には、以下に述べるような問題がある。第１の方法では、すべての共通鍵を保管しておくようにするので、不特定多数のユーザがエンティティとなって暗号通信を行うネットワーク社会には適さない。また、第２の方法は、鍵共有のための予備通信が必要である点が問題である。

【０００７】第３の方法は、予備通信が不要であり、公開された相手の特定情報（ＩＤ情報）とセンタから予め配布されている固有の秘密パラメータとを用いて、任意の相手との共通鍵を生成できるので、便利な方法である。しかしながら、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【０００８】この結託問題の難しさは、特定情報（ＩＤ情報）に基づく秘密パラメータがセンタ秘密と個人秘密

との二重構造になっていることに起因する。第３の方法では、センタの公開パラメータと個人の公開された特定情報（ＩＤ情報）とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【０００９】

【発明が解決しようとする課題】そこで、本発明者等は、特定情報（ＩＤ情報）をいくつかに分割し、複数の各センタからその分割した特定情報（ＩＤ情報）に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる秘密鍵生成方法，暗号化方法及び暗号通信方法を提案している｛特願平11－16257号，特願平11－59049 号（以下、これらを先行例という）｝。

【００１０】結託問題を解決することを目的として提案されてきたエンティティの特定情報（ＩＤ情報）に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報（ＩＤ情報）をいくつかに分割し、分割した各特定情報（各ＩＤ情報）についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【００１１】この先行例の提案方法では、信頼される複数のセンタが設けられ、各センタは各エンティティの分割した１つの特定情報（ＩＤ情報）に対応する数学的構造を持たない秘密鍵を生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ＩＤ情報）とから共通鍵を、予備通信を行わずに生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【００１２】そして、本発明者等は、エンティティの特定情報（ＩＤ情報）の分割を利用したこの提案方法の改良を研究し続けている。特に、複数のエンティティが結託して彼らの秘密鍵のすべてを用いて特定のエンティティを攻撃するという結託攻撃に強い改良方法を研究している。

【００１３】本発明は斯かる事情に鑑みてなされたものであり、上記提案方法を改良して結託攻撃に対してより強くした秘密鍵生成方法及び暗号化方法を提供することを目的とする。

【００１４】

【課題を解決するための手段】請求項１に係る秘密鍵生成方法は、エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて前記秘密鍵を生成することを特徴とする。

【００１５】請求項２に係る暗号化方法は、各エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて各エンティティ固有の秘密鍵を生成することを特徴とする。

【００１６】請求項３に係る秘密鍵生成方法は、エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、前記分割特定情報の各ブロックを誤り訂正符号の符号語で構成することを特徴とする。

【００１７】先行例の提案方法では、エンティティの特定情報（ＩＤ情報）を分割した分割特定情報（分割ＩＤ情報）を示す各分割ベクトルにおいて個人秘密乱数が一定であって、その分割ベクトル内の各成分における個人秘密乱数の値が同じであるので、結託攻撃を受ける可能性があった。そこで、本発明では、各分割ベクトルにおいて個人秘密乱数を一定とせず、その分割ベクトル内の各成分に対して相異なる個人秘密乱数を設定しており、結託攻撃に対してより強くできる。

【００１８】また、本発明では、分割特定情報（分割ＩＤ情報）を示す各分割ベクトルを誤り訂正符号の符号語で構成する。よって、この符号語に基づく特定情報（ＩＤ情報）の分割を、上記の個人秘密乱数の多様化方式に組み合わせることにより、結託攻撃に対して更なる強化を図れる。

【００１９】

【発明の実施の形態】図１は、各エンティティの特定情報（ＩＤ情報）を複数のブロックに分割した分割特定情報を利用するＩＤ－ＮＩＫＳ方式を採用した本発明及び先行例における暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｊ個）のセンタ１が設定されており、これらのセンタ１としては、例えば社会の公的機関を該当できる。

【００２０】これらの各センタ１と、この暗号系システムを利用するユーザとしての複数の各エンティティａ，

5　　6

b，…，ｚとは、秘密通信路2_{a1}，…，2_{aJ}、2_{b1}，…，2_{bJ}、・・・、2_{z1}，…，2_{zJ}により接続されており、これらの秘密通信路を介して各センタ１から秘密の鍵情報が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００２１】まず、本発明による改良対象の一例となる先行例の１つ（特願平11－59049 号）に示されている暗号通信方式について説明する。

【００２２】（センタ１での準備処理）センタ１は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　N　　N＝PQ

　　J　　ＩＤベクトルの分割ブロック数

　　M_j　　分割したＩＤベクトルのサイズ（ｊ＝１，２，・・・，Ｊ）

　　L　　ＩＤベクトルのサイズ（$L=M_1+M_2+\cdots+M_J$）

　　T　　指数部分の次数

秘密鍵　P，Q　　大きな素数

　　g　　Ｎを法とする最大生成元

　　H_j　　乱数からなる$2^{Mj}\times 2^{Mj}$の対称行列

　　α_e　　エンティティｅの個人秘密乱数

　　（但し、ｇｃｄ（α_e，λ（Ｎ））＝１，

　　λ（・）はカーマイケル関数）

　　β_{ej}　　エンティティｅの個人秘密乱数

　　（但し、$\beta_{e1}+\beta_{e2}+\cdots+\beta_{eJ}=\lambda$（Ｎ））

【００２３】各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図２に示すようにそのＩＤベクトルをブロックサイズM_1，M_2，・・・，M_J毎にＪ個のブロックに分割する。例えば、エンティティｅのＩＤベクトル（ベクトルI_e）を式（１）のように分割する。分割特定情報である各ベクトルI_{ej}（ｊ＝１，２，・・・，Ｊ）をＩＤ分割ベクトルと呼ぶ。

【００２４】

【数１】

$$\overrightarrow{I_e}=[\overrightarrow{I_{e1}}\,|\,\overrightarrow{I_{e2}}\,|\cdots|\,\overrightarrow{I_{eJ}}]\quad\cdots(1)$$

【００２５】（エンティティの登録処理）エンティティｅに登録を依頼された各センタ１は、準備した鍵とエンティティｅのＪ個のＩＤ分割ベクトルについて、それぞれに対応するＪ個の秘密鍵ベクトルs_{ej}（ｊ＝１，２，・・・，Ｊ）を以下の式（2-1），（2-2），・・・，（2-j），・・・，（2-J)に従って計算する。

【００２６】

【数２】

$$\overrightarrow{s_{e1}}=\alpha_e H_1[\overrightarrow{I_{e1}}]+\beta_{e1}\overrightarrow{1}\quad\cdots(2-1)$$

$$\overrightarrow{s_{e2}}=\alpha_e H_2[\overrightarrow{I_{e2}}]+\beta_{e2}\overrightarrow{1}\quad\cdots(2-2)$$

$$\vdots$$

$$\overrightarrow{s_{ej}}=\alpha_e H_j[\overrightarrow{I_{ej}}]+\beta_{ej}\overrightarrow{1}\quad\cdots(2-j)$$

$$\vdots$$

$$\overrightarrow{s_{eJ}}=\alpha_e H_J[\overrightarrow{I_{eJ}}]+\beta_{eJ}\overrightarrow{1}\quad\cdots(2-J)$$

【００２７】但し、ベクトル１は、すべての成分が１であるＪ次元のベクトルを表す。また、H_j［ベクトルI_{ej}］は対称行列$H_j=(k_{em}^{(j)})$からベクトルI_{ej}に対応した行を１行抜き出したものを表し、［・］の操作を参照と定義する。

【００２８】次に、第１ブロックに関して、（Ｔ＋１）個の秘密鍵ベクトルg_{et}（ｔ＝０，１，２，・・・，Ｔ）を以下の式（3-0），（3-1），（3-2），・・・，（3-t），・・・，（3-T)に従って計算する。

【００２９】

【数３】

7 8

$$\overrightarrow{g_{e0}} \equiv g^{\alpha_e^{-T}\cdot 1} \pmod N \quad \cdots(3\text{-}0)$$

$$\overrightarrow{g_{e1}} \equiv g^{\alpha_e^{-T}\overrightarrow{s_{e1}}} \pmod N \quad \cdots(3\text{-}1)$$

$$\overrightarrow{g_{e2}} \equiv g^{\alpha_e^{-T}\langle\overrightarrow{s_{e1}}\rangle^2} \pmod N \quad \cdots(3\text{-}2)$$

$$\vdots$$

$$\overrightarrow{g_{et}} \equiv g^{\alpha_e^{-T}\langle\overrightarrow{s_{e1}}\rangle^t} \pmod N \quad \cdots(3\text{-}t)$$

$$\vdots$$

$$\overrightarrow{g_{eT}} \equiv g^{\alpha_e^{-T}\langle\overrightarrow{s_{e1}}\rangle^T} \pmod N \quad \cdots(3\text{-}T)$$

【００３０】但し、ｃをスカラー、（４），（５）に示すＡ，Ｂを行列とした場合、Ｂ＝ｃ^{A} 及びＢ＝〈Ａ〉^{c} は、それぞれ（６）及び（７）を表す。

【００３１】

【数４】

$$A=(a_{\mu\nu}) \quad \cdots(4)$$

$$B=(b_{\mu\nu}) \quad \cdots(5)$$

$$b_{\mu\nu}=c^{a_{\mu\nu}} \quad \cdots(6)$$

$$b_{\mu\nu}=a_{\mu\nu}c \quad \cdots(7)$$

【００３２】そして、１つのセンタ１は、第１ブロックに関する（Ｔ＋１）個の秘密鍵ベクトルg_{et}（ｔ＝０，１，２，・・・，Ｔ）を秘密裏にエンティティｅへ送り、残りの（Ｊ－１）の各センタ１は、第２ブロック以降に関する（Ｊ－１）個の秘密鍵ベクトルs_{ej}（ｊ＝２，３，・・・，Ｊ）を秘密裏にエンティティｅへ送る。

【００３３】（エンティティ間の共通鍵の生成処理）エンティティｅは、第１ブロックに関して、自身の（Ｔ＋１）個の秘密鍵ベクトルg_{et}の中から、通信相手のエンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルg_{et}［ベクトルI_{m1}］を選び出す。この選び出したものを(8-0)，(8-1)，・・・，(8-t)，・・・，(8-T)に示す。

【００３４】

【数５】

$$g_{0em}=\overrightarrow{g_{e0}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}0)$$

$$g_{1em}=\overrightarrow{g_{e1}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}1)$$

$$\vdots$$

$$g_{tem}=\overrightarrow{g_{et}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}t)$$

$$\vdots$$

$$g_{Tem}=\overrightarrow{g_{eT}}[\overrightarrow{I_{m1}}] \quad \cdots(8\text{-}T)$$

【００３５】次に、エンティティｅは、ｊ＝２，３，・・・，Ｊの第２，第３，・・・，第Ｊの各ブロックに関して、自身の秘密鍵ベクトルs_{ej}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{mj}に対応する成分のベクトルs_{ej}［ベクトルI_{mj}］を各ブロック毎に選び出す。この選び出したものを(9-2)，・・・，(9-j)，・・・，(9-J)に示す。

【００３６】

【数６】

$$x_{2em}=\overrightarrow{s_{e2}}[\overrightarrow{I_{m2}}] \quad \cdots(9\text{-}2)$$

$$\vdots$$

$$x_{jem}=\overrightarrow{s_{ej}}[\overrightarrow{I_{mj}}] \quad \cdots(9\text{-}j)$$

$$\vdots$$

$$x_{Jem}=\overrightarrow{s_{eJ}}[\overrightarrow{I_{mJ}}] \quad \cdots(9\text{-}J)$$

【００３７】更に、（10）のように整数環上でこれらのすべての和y_{em}を求める。

【００３８】

【数７】

$$y_{em}=\sum_{j=2}^{J} x_{jem} \quad \cdots(10)$$

【００３９】そして、Ｎを法として以下の（11）のような計算を行うことにより、共通鍵K_{em}を求める。この（11）の計算において、全ブロックの計算を完了することにより、個人秘密乱数α_eはその逆元との乗算にて消去され、Ｊ個の個人秘密乱数β_{ej}はそれらの加算にて消去される。このK_{em}はエンティティｍ側から求めた共通鍵K_{me}と一致する。

【００４０】

【数８】

9　　10

$$K_{em} \equiv \prod_{t=0}^{T} g_{t\,em}^{\;T C_t \gamma_{em}^{(T-t)}}$$
$$\equiv g^{\alpha_e^{-T} \sum_{t=0}^{T} {}_T C_t x_{1em}^{t} \gamma_{em}^{T-t}}$$
$$\equiv g^{\alpha_e^{-T} (x_{1em} + \gamma_{em})^T}$$
$$\equiv g^{\alpha_e^{-T} (x_{1em} + \cdots + x_{Jem})^T}$$
$$\equiv g^{\alpha_e^{-T} (\alpha_e H_1 [\overrightarrow{I_{e1}}][\overrightarrow{I_{m1}}] + \beta_{e1} + \cdots + \alpha_e H_J [\overrightarrow{I_{eJ}}][\overrightarrow{I_{mJ}}] + \beta_{eJ})^T}$$
$$\equiv g^{\alpha_e^{-T} \{\alpha_e (H_1 [\overrightarrow{I_{e1}}][\overrightarrow{I_{m1}}] + \cdots + H_J [\overrightarrow{I_{eJ}}][\overrightarrow{I_{mJ}}]) + \lambda(N)\}^T}$$
$$\equiv g^{\alpha_e^{-T} \{\alpha_e (H_1 [\overrightarrow{I_{e1}}][\overrightarrow{I_{m1}}] + \cdots + H_J [\overrightarrow{I_{eJ}}][\overrightarrow{I_{mJ}}])\}^T}$$
$$\equiv g^{(H_e [\overrightarrow{I_{e1}}][\overrightarrow{I_{m1}}] + \cdots + H_J [\overrightarrow{I_{eJ}}][\overrightarrow{I_{mJ}}])^T} \pmod N$$

・・・(11)

【００４１】なお、上式においてx_{1em}　＝ベクトルs_{e1}［ベクトルI_{m1}］と置いたが、これは、エンティティｅ自身にもわからない。また、Ｔは比較的小さな数であるので、指数部分はべき乗を順次繰り返し行うことにより計算することができる。

【００４２】なお、上記例において、各ブロックのサイズM_Jは全ブロックにおいて一定であっても良いし、その一部または全部のブロックで異なっていても良い。しかし、第１ブロックに関して秘密鍵ベクトルg_{et}を求めるので、全ブロックについてそのサイズを一定にした場合、第１ブロックについての秘密が大きくなってしまう。よって、第１ブロックのサイズを他のブロックのサイズよりも小さくするようにした方が良い。特に、M_1＝１とした場合、配布する秘密を最小限にすることができ、最も安全性が高くなる。

【００４３】以下、上記先行例と対比しながら、本発明の特徴部分について説明する。上述した先行例では、各ＩＤ分割ベクトル（各ブロック）においてエンティティｅの個人秘密乱数β_{ej}（ｊ＝１，２，・・・，Ｊ）が一定であり、その各ＩＤ分割ベクトル内の各成分における個人秘密乱数β_{ej}の値を同じに設定している。よって、各ブロック内で隣合ったもの同士を減算することによって、この個人秘密乱数β_{ej}を消去できる攻撃が考えられる。

【００４４】そこで、本発明では、各分割ベクトル（各ブロック）において個人秘密乱数を一定とせず、その分割ベクトル内の各成分に対して相異なる個人秘密乱数$\beta_{ej}^{(v)}$（ｊ＝１，２，・・・，Ｊ、ｖ＝０，１，・・・，$2^{M_J}-1$）を設定する。

【００４５】本発明では、センタ１で、以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵　Ｎ　　Ｎ＝ＰＱ
　　Ｊ　　ＩＤベクトルの分割ブロック数
　　M_J　　分割したＩＤベクトルのサイズ（ｊ＝１，２，・・・，Ｊ）
　　Ｌ　　ＩＤベクトルのサイズ（$L=M_1+M_2+\cdots+M_J$）
　　Ｔ　　指数部分の次数
秘密鍵　Ｐ，Ｑ　　大きな素数
　　ｇ　　Ｎを法とする最大生成元
　　H_J　　乱数からなる$2^{M_J} \times 2^{M_J}$の対称行列
　　α_e　　エンティティｅの個人秘密乱数
　　（但し、ｇｃｄ（α_e，λ（Ｎ））＝１，
　　λ（・）はカーマイケル関数）
　　$\beta_{ej}^{(v)}$　　エンティティｅの個人秘密乱数
　　（ｖ＝０，１，・・・，M_J-1）
　　（但し、$\gamma_{eR1}+\gamma_{eR2}+\cdots+\gamma_{eRK}=n\lambda(N)$（ｎ：整数）。全Ｊ個の分割ブロックを１個または複数個のブロックを１組としてＫ組に組分けしており、即ち、R_KはＪ以下の自然数を要素とする全体集合（Ｕ）の部分集合であって、任意のｐ，ｑにおいて$R_p \cap R_q$

は空集合、$R_1 \cup R_2 \cup \cdots \cup R_K$ は全体集合（U）である。また、γ_{eRk} は、R_k に該当するブロック（分割ベクトル）内の各成分における個人秘密乱数と補正項とを演算して一定値としたものである。）

【００４６】なお、部分集合R_K の作り方は、各エンティティにおいて異なっていても良いことは勿論である。また、１つの部分集合R_K における要素の個数も任意であって良い。

【００４７】上述した先行例と同様、前記式（１）のように、エンティティｅのＩＤベクトル（ベクトルI_e）を分割する。そして、各センタ１は、準備した鍵とエンティティｅのＪ個のＩＤ分割ベクトルについて、それぞれに対応するＪ個の秘密鍵ベクトルs_{ej}（ｊ＝１，２，・・・，Ｊ）を計算する。ここで、本発明では、ｊ番目のセンタからエンティティｅへ配布される秘密鍵ベクトルs_{ej}において、各成分毎に異なる乱数を用いており、２ブロック目以降のベクトルs_{ej}は、一般化した形で以下の式（12-2），（12-3），・・・，（12-J）で与える。なお、以下の例では、各ブロックのサイズをM_j＝１としている。本発明の式（12-2），（12-J）は、先行例の式（２-2），（２-J）にそれぞれ対応している。

【００４８】

【数９】

$$\overrightarrow{s_{e2}}(\beta_2^{(0)},\beta_2^{(1)}) = (\alpha_e k_{e2_1}^{(2)} + \beta_{e2}^{(0)}, \alpha_e k_{e2_2}^{(2)} + \beta_{e2}^{(1)}) \quad \cdots (12\text{-}2)$$

$$\overrightarrow{s_{e3}}(\beta_3^{(0)},\beta_3^{(1)}) = (\alpha_e k_{e3_1}^{(3)} + \beta_{e3}^{(0)}, \alpha_e k_{e3_2}^{(3)} + \beta_{e3}^{(1)}) \quad \cdots (12\text{-}3)$$

$$\vdots$$

$$\overrightarrow{s_{eJ}}(\beta_J^{(0)},\beta_J^{(1)}) = (\alpha_e k_{eJ_1}^{(J)} + \beta_{eJ}^{(0)}, \alpha_e k_{eJ_2}^{(J)} + \beta_{eJ}^{(1)}) \quad \cdots (12\text{-}J)$$

【００４９】このようにした場合、乱数の総和$\beta_{e2}+\beta_{e3}+\cdots+\beta_{eJ}$は$2^{J-1}$通りの値をとるので、比較的小さなＪ、例えばＪ＝21としても、その数は$2^{20} \fallingdotseq 10^6$となり、実用上の大きな障害になってしまう。そこで、Ｓブロック毎に2^S通りに広がる乱数値$\beta_{e1}+\cdots+\beta_{e,1+S-1}$を一定値に変換することを考える。

【００５０】体F_2上のＩＤベクトルを一般的に以下（13）のように表す。

$ID_2 = (b_1, b_2, \cdots, b_J)$　　…（13）

ここで、Ｓ＝２とし、２ビットでペアを考える。なお、任意のペアを一般に（b_1，b_J）と表記する。また、すべてのペアで重複なく全体を覆うものとし、ペアの組合せ（上記R_kのパターン）はエンティティｅに教えることとする。

【００５１】そして、部分和S_{bibj}に対し、乱数値を一定値γ_{eij}に変換するために補正項C_{bibj}を以下のように加算する。但し、すべてのペア（ｉ，ｊ）について、γ_{e1j}を加算するとλ（Ｎ）となるようにγ_{eij}を決める。まず、S_{bibj}，C_{bibj}は（b_1 b_J）の値により、それぞれ以下の式（14），（15）のように４通りで与えられる。

【００５２】

【数１０】

$$\left.\begin{aligned} S_{00} &= \alpha_e k_{e_i 1}^{(i)} + \alpha_e k_{e_j 1}^{(j)} + \beta_{ei}^{(0)} + \beta_{ej}^{(0)} \\ S_{01} &= \alpha_e k_{e_i 1}^{(i)} + \alpha_e k_{e_j 2}^{(j)} + \beta_{ei}^{(0)} + \beta_{ej}^{(1)} \\ S_{10} &= \alpha_e k_{e_i 2}^{(i)} + \alpha_e k_{e_j 1}^{(j)} + \beta_{ei}^{(1)} + \beta_{ej}^{(0)} \\ S_{11} &= \alpha_e k_{e_i 2}^{(i)} + \alpha_e k_{e_j 2}^{(j)} + \beta_{ei}^{(1)} + \beta_{ej}^{(1)} \end{aligned}\right\} \cdots (14)$$

$$\left.\begin{aligned} C_{00} &= \gamma_{eij} - (\beta_{ei}^{(0)} + \beta_{ej}^{(0)}) \\ C_{01} &= \gamma_{eij} - (\beta_{ei}^{(0)} + \beta_{ej}^{(1)}) \\ C_{10} &= \gamma_{eij} - (\beta_{ei}^{(1)} + \beta_{ej}^{(0)}) \\ C_{11} &= \gamma_{eij} - (\beta_{ei}^{(1)} + \beta_{ej}^{(1)}) \end{aligned}\right\} \cdots (15)$$

【００５３】従って、S_{b1bj} ＋C_{b1bj} は以下の式（16）のように与えられる。

【００５４】

【数１１】

$$\left.\begin{aligned} S_{00}+C_{00} &= \alpha_e k_{e_i1}^{(i)} + \alpha_e k_{e_j1}^{(j)} + \gamma_{eij} \\ S_{01}+C_{01} &= \alpha_e k_{e_i1}^{(i)} + \alpha_e k_{e_j2}^{(j)} + \gamma_{eij} \\ S_{10}+C_{10} &= \alpha_e k_{e_i2}^{(i)} + \alpha_e k_{e_j1}^{(j)} + \gamma_{eij} \\ S_{11}+C_{11} &= \alpha_e k_{e_i2}^{(i)} + \alpha_e k_{e_j2}^{(j)} + \gamma_{eij} \end{aligned}\right\} \cdots (16)$$

【００５５】第１ブロックに関しては、上述した先行例と同様に、（Ｔ＋１）個の秘密鍵ベクトルg_{et}（ｔ＝０，１，２，・・・，Ｔ）を計算する。そして、１つのセンタ１は、第１ブロックに関する（Ｔ＋１）個の秘密鍵ベクトルg_{et}（ｔ＝０，１，２，・・・，Ｔ）を秘密裏にエンティティｅへ送り、残りの（Ｊ－１）の各センタ１は、第２ブロック以降に関する（Ｊ－１）個の秘密鍵ベクトルs_{ej}（ｊ＝２，３，・・・，Ｊ）を秘密裏にエンティティｅへ送る。

【００５６】エンティティｅは、上述した先行例と同様に、第１ブロックに関して、自身の（Ｔ＋１）個の秘密鍵ベクトルg_{et}の中から、通信相手のエンティティｍのＩＤ分割ベクトルであるベクトルI_{m1}に対応する成分のベクトルg_{et}［ベクトルI_{m1}］を選び出す。次に、エンティティｅは、第２，第３，・・・，第Ｊの各ブロックに関して、自身の秘密鍵ベクトルs_{ej}の中から、エンティティｍのＩＤ分割ベクトルであるベクトルI_{mj}に対応する成分のベクトルs_{ej}［ベクトルI_{mj}］を各ブロック毎に選び出し、整数環上でこれらのすべての和y_{em}を求める。

【００５７】そして、上述した先行例と同様に、Ｎを法として共通鍵K_{em}を求める。この際、個人秘密乱数α_eがその逆元との乗算にて消去され同じであり、また、本発明ではγ_{eR1} ＋γ_{eR2} ＋・・・＋γ_{eRK} ＝ｎλ（Ｎ）に設定されているので、個人秘密乱数$\beta_{ej}^{(v)}$はそれらの加算にて消去される。

【００５８】このように秘密鍵を生成した場合に、本発明が結託攻撃に強いことを以下に説明する。上記式（16）からγ_{eij}を消去すると、d_{e1}～d_{e3}を適当な定数として、以下の式（17）で示される関係が得られる。式（17）において独立な式は明らかに２個である。

【００５９】

【数１２】

$$\left.\begin{aligned} \alpha_e k_{e_i1}^{(i)} - \alpha_e k_{e_i2}^{(i)} &= d_{e1} \\ \alpha_e k_{e_j1}^{(j)} - \alpha_e k_{e_j2}^{(j)} &= d_{e2} \\ \alpha_e k_{e_i1}^{(i)} - \alpha_e k_{e_i2}^{(i)} + \alpha_e k_{e_j1}^{(j)} - \alpha_e k_{e_j2}^{(j)} &= d_{e3} \end{aligned}\right\} \cdots (17)$$

【００６０】ここで、ペア（b_i，b_j）に関わる行列の要素$k_{ei1}^{(i)}$，$k_{ei2}^{(i)}$，$k_{ej1}^{(j)}$，$k_{ej2}^{(j)}$を知るためにN_T人が結託したとする。独立な式は（４N_T＋２）個であり、これに対する未知数は、α_eを定数と考えたとしても、（４N_T＋４）個となって、未知数の個数が方程式の個数を上回る。この結果、各要素$k_{ei1}^{(i)}$，$k_{ei2}^{(i)}$，$k_{ej1}^{(j)}$，$k_{ej2}^{(j)}$は露呈しない。

【００６１】また、本発明の方式における安全性について説明する。安全なＩＤ－ＮＩＫＳの必要条件として、秘密鍵生成関数及び鍵共有関数が多項式時間で分離できないことが知られている。以下に、この方式がこれらの安全性の必要条件を満たすことを示す。

【００６２】（秘密鍵生成関数）本発明の方式は、式（18），（19）に示すＪ個の秘密鍵生成関数を有する。

【００６３】

【数１３】

$$f_1(\vec{x}) = g^{\alpha_{e1} H_1[\vec{x}]} \quad (J=1) \cdots (18)$$

$$f_j(\vec{x}) = \alpha_{ej} H_j[\vec{x}] \quad (j=2,\ldots,J) \cdots (19)$$

【００６４】Ｈを任意の対称行列した場合、式（20），（21）に示すように、参照関数［・］は明らかに分離不可能である。

【００６５】

【数１４】

15

$$H[\vec{x}+\vec{y}]\neq H[\vec{x}]+H[\vec{y}] \quad \cdots(20)$$

$$H[\vec{x}+\vec{y}]\neq H[\vec{x}]\cdot H[\vec{y}] \quad \cdots(21)$$

【００６６】従って、前記式（18），（19）で表される

$$f_j(\vec{x}+\vec{y})\neq f_j(\vec{x})\circ f_j(\vec{y}) \quad (j=1,2,\ldots,J) \quad \cdots(22)$$

【００６８】（鍵共有関数）この方式における鍵共有関数を、式（23）に示す。

$$F(\vec{x},\vec{y})=g\,H_1[\vec{x}_1][\vec{y}_1]\cdots H_K[\vec{x}_K][\vec{y}_K] \quad \cdots(23)$$

【００７０】秘密鍵生成関数の場合と同様に、式（23）で表される鍵共有関数は、式（24）に示すように、分離不可能である。

$$F(\vec{a},\vec{x}+\vec{y})\neq F(\vec{a},\vec{x})\circ F(\vec{a},\vec{y}) \quad \cdots(24)$$

【００７２】ところで、上述した方式にあっては、$\alpha_e(k_{ei1}^{(i)}-k_{ei2}^{(i)})$，$\alpha_e(k_{ej1}^{(j)}-k_{ej2}^{(j)})$の形は露呈する。そこで、$\alpha_e(k_{ei1}^{(i)}-k_{ei2}^{(i)})$などの形では露呈しないような手法について、以下に説明する。

【００７３】この手法では、分割ＩＤベクトルを誤り訂正符号の符号語で構成している。例えば、２次元ＩＤベクトルID_2の連続する２つの成分b_{2n}，b_{2n+1}（$n=1,2,\cdots,J$）に対し、以下の式（25）を満たす成分c_n'をb_{2n+1}の後に挿入し、b_{2n}，b_{2n+1}，c_n'で符号語を構成するようにする。c_n'挿入後のベクトルを以下の（26）のようにID_2'と表記する。

$$b_{2n}+b_{2n+1}=c_n' \pmod 2 \quad \cdots(25)$$

$$ID_2'=(b_1,b_2,b_3,c_1',b_4,b_5,c_2',\cdots,b_{2J},b_{2J+1},c_J') \quad \cdots(26)$$

【００７４】$\{(b_{2n},b_{2n+1},c_n')\}$は符号長ｎ＝３，情報記号数ｋ＝２，最小距離ｄ＝２の線形符号となる。よって、上述した方式の場合と同様の議論により、d_{e4}～d_{e6}を適当な定数として、以下の式（27）が導かれる。これらの中で独立な式は２個しかない。従って、個々の$\alpha_e(k_{ei1}^{(i)}-k_{ei2}^{(i)})$などは明らかに露呈しない。

$$\left.\begin{aligned}\alpha_e(k_{ei1}^{(i)}-k_{ei2}^{(i)})+\alpha_e(k_{ej1}^{(j)}-k_{ej2}^{(j)})&=d_{e4}\\ \alpha_e(k_{ei1}^{(i)}-k_{ei2}^{(i)})+\alpha_e(k_{ek1}^{(k)}-k_{ek2}^{(k)})&=d_{e5}\\ \alpha_e(k_{ej1}^{(j)}-k_{ej2}^{(j)})+\alpha_e(k_{ek1}^{(k)}-k_{ek2}^{(k)})&=d_{e6}\end{aligned}\right\} \quad \cdots(27)$$

【００７６】よって、分割ＩＤベクトルを誤り訂正符号の符号語で構成するこのような分割ＩＤベクトル作成方式に、個人秘密乱数を分割ＩＤベクトルの各成分毎に異ならせる上述したような乱数多様化方式を組み合わせることにより、より安全な暗号通信システムを構築することが可能である。

【００７７】次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図３は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図３の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ伝送し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

16

Ｊ個の秘密鍵生成関数は、式（22）に示すように、分離不可能である。

【００６７】

【数１５】

【００６９】

【数１６】

【００７０】

【００７１】

【数１７】

【００７５】

【数１８】

【００７８】１番目のセンタ１には、各エンティティａ，ｂ固有の秘密鍵ベクトルs_{a1}，s_{b1}と（Ｔ＋１）個の秘密鍵ベクトルg_{at}，g_{bt}（$t=0,1,2,\cdots,T$）とを計算する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルg_{at}，g_{bt}がエンティティａ，ｂへ送付される。

【００７９】ｊ（ｊ＝２，３，・・・，Ｊ）番目のセンタ１には、各エンティティａ，ｂ固有の秘密鍵ベクトル

s_{aj}，s_{bj}を計算する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵ベクトルs_{aj}，s_{bj}がエンティティａ，ｂへ送付される。

【００８０】エンティティａ側には、各センタ１から送られるこれらの秘密鍵ベクトルg_{at}（ｔ＝０，１，２，・・・，Ｔ），s_{aj}（ｊ＝２，３，・・・，Ｊ）をテーブル形式で格納しているメモリ１０と、これらの秘密鍵ベクトルの中からエンティティｂに対応する成分であるベクトルg_{at}［ベクトルI_{bl}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{aj}［ベクトルI_{bj}］（ｊ＝２，３，・・・，Ｊ）を選び出す成分選出器１１と、選び出されたこれらの成分を使用してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００８１】また、エンティティｂ側には、各センタ１から送られるこれらの秘密鍵ベクトルg_{bt}（ｔ＝０，１，２，・・・，Ｔ），s_{bj}（ｊ＝２，３，・・・，Ｊ）をテーブル形式で格納しているメモリ２０と、これらの秘密ベクトルの中からエンティティａに対応する成分であるベクトルg_{bt}［ベクトルI_{al}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{bj}［ベクトルI_{aj}］（ｊ＝２，３，・・・，Ｊ）を選び出す成分選出器２１と、選び出されたこれらの成分を使用してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路30から入力した暗号文Ｃを平文Ｍに復号して出力する復号器２３とが備えられている。

【００８２】エンティティａからエンティティｂへ情報を伝送しようとする場合、まず、各センタ１で求められて、予めメモリ１０に格納されている秘密鍵ベクトルg_{at}（ｔ＝０，１，２，・・・，Ｔ），s_{aj}（ｊ＝２，３，・・・，Ｊ）が成分選出器１１へ読み出される。そして、成分選出器11にて、エンティティｂに対応する成分であるベクトルg_{at}［ベクトルI_{bl}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{aj}［ベクトルI_{bj}］（ｊ＝２，３，・・・，Ｊ）が選び出されて共通鍵生成器１２へ送られる。共通鍵生成器１２にて、これらの成分を使用して（11）に従って共通鍵K_{ab}が求められ、暗号化器１３へ送られる。暗号化器１３において、この共通鍵K_{ab}を用いて平文Ｍが暗号文Ｃに暗号化され、暗号文Ｃが通信路３０を介して伝送される。

【００８３】通信路３０を伝送された暗号文Ｃはエンティティｂの復号器２３へ入力される。各センタ１で求められて、予めメモリ２０に格納されている秘密鍵ベクトルs_{bj}（ｊ＝２，３，・・・，Ｊ），g_{bt}（ｔ＝０，１，２，・・・，Ｔ）が成分選出器２１へ読み出される。そして、成分選出器２１にて、エンティティａに対応する成分であるベクトルg_{bt}［ベクトルI_{al}］（ｔ＝０，１，２，・・・，Ｔ），ベクトルs_{bj}［ベクトルI_{aj}］（ｊ＝２，３，・・・，Ｊ）が選び出されて共通鍵生成器２２へ送られる。共通鍵生成器２２にて、これらの成分を使用して（11）に従って共通鍵K_{ba}が求められ、復号器２３へ送られる。復号器２３において、この共通鍵K_{ba}を用いて暗号文Ｃが平文Ｍに復号される。

【００８４】このような例では、複数のセンタが設けられ、各センタはエンティティの分割した１つのＩＤ情報に対応する鍵を生成するようにしたので、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。また、各エンティティ固有の秘密鍵ベクトルが予めエンティティ側のメモリに格納されているので、共通鍵生成に要する時間が短くて済む。

【００８５】図４は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各エンティティの特定情報（ＩＤ情報）を分割してＩＤ分割ベクトルを得る分割処理と、各エンティティにおける秘密鍵ベクトルs_{ej}，g_{et}を求める秘密鍵生成処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各センタ側に設けられている。

【００８６】図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各センタにおいて上述の分割処理と秘密鍵生成処理とを実行する。

【００８７】コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各センタにおいて上述の分割処理と秘密鍵生成処理とを実行する。

【００８８】コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、各センタにおいて上述の分割処理と秘密鍵生成処理とを実行する。

【００８９】なお、上述した例では、特願平11－59049号に示された秘密鍵の生成方式に本発明を適用する場合について説明したが、分割ＩＤベクトルと個人秘密乱数βとを用いて秘密鍵を生成するようにした他のＩＤ－Ｎ

ＩＫＳ方式（例えば特願平11－16257 号で開示した方式）についても、本発明を同様に適用できることは勿論である。

【００９０】

【発明の効果】以上のように、本発明では、各分割ベクトルにおいて個人秘密乱数を一定とせず、その分割ベクトル内の各成分に対して相異なる個人秘密乱数を設定するようにしたので、結託攻撃に対してより強くできる。

【００９１】また、本発明では、各分割ベクトルを誤り訂正符号の符号語で構成するようにしたので、このような分割ベクトルの形成方式を上記の個人秘密乱数の多様化方式に組み合わせることにより、結託攻撃に対して更なる強化を図れる。

【００９２】（付記）なお、以上の説明に対して更に以下の項を開示する。

（１）　エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて前記秘密鍵を生成することとし、前記分割ベクトルの分割ブロック数をＪ、前記分割ベクトルの各サイズをM_j　（ｊ＝１，２，・・・，Ｊ）、エンティティｅの個人秘密乱数を$\beta_{ej}^{(v)}$　（ｖ＝０，１，・・・，M_j －１）とした場合に、全Ｊ個の分割ブロックを１または複数個のブロックを１組としてＫ組に組分けしており、γ_{eR1} ＋γ_{eR2} ＋・・・＋γ_{eRK} ＝ｎλ（Ｎ）（ｎ：整数、λ（・）：カーマイケル関数、Ｎ＝ＰＱ（Ｐ，Ｑは素数））を満たす秘密鍵生成方法。

但し、R_k ：Ｊ以下の自然数を要素とする全体集合（Ｕ）の部分集合（任意のｐ，ｑにおいて$R_p \cap R_q$ は空集合、$R_1 \cup R_2 \cup \cdots \cup R_K$ は全体集合（Ｕ））

γ_{eRk} ：S_k に該当する分割ベクトル内の各成分における個人秘密乱数と補正項とを演算して得られる一定値

【００９３】（２）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと、分割された各ブロック毎に設定された各エンティティ固有の個人秘密乱数とを用いて、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記分割ベクトルの各成分毎にその値を異ならせて前記個人秘密乱数を設定し、その設定した個人秘密乱数と前記分割ベクトルとを用いて各エンティティ固有の秘密鍵を生成する暗号通信方法。

【００９４】（３）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行う暗号通信システムにおいて、各エンティティの特定情報を複数のブロックに分割した分割特定情報を示す分割ベクトルと該分割ベクトルの各成分毎にその値を異ならせて設定した個人秘密乱数とを利用して、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵に含まれている、通信対象のエンティティの分割特定情報に対応する成分を使用して、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システム。

【００９５】（４）　コンピュータに、暗号通信システムにおける各エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、各エンティティの特定情報を複数のブロックに分割して分割ベクトルを得ることをコンピュータに実行させるプログラムコード手段と、前記分割ベクトルと前記分割ベクトルのの各成分毎にその値を異ならせて設定した個人秘密乱数とを利用して、各エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【００９６】（５）　各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、前記分割特定情報の各ブロックを誤り訂正符号の符号語で構成して各エンティティ固有の秘密鍵を生成する暗号化方法。

【００９７】（６）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティ

ティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記分割特定情報の各ブロックを誤り訂正符号の符号語で構成して各エンティティ固有の秘密鍵を生成する暗号通信方法。

【００９８】（７）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行う暗号通信システムにおいて、各エンティティの特定情報が、各ブロックが誤り訂正符号の符号語で構成されるように、複数のブロックに分割された分割特定情報を利用して、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵に含まれている、通信対象のエンティティの分割特定情報に対応する成分を使用して、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システム。

【００９９】（８）　コンピュータに、暗号通信システムにおける各エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、各エンティティの特定情報を、各ブロックが誤り訂正符号の符号語で構成されるように、複数のブロックに分割して分割特定情報を得ることをコンピュータに実行させるプログラムコード手段と、前記分割特定情報を利用して、各エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】本発明の暗号通信システムの構成を示す模式図である。

【図２】エンティティのＩＤベクトルの分割例を示す模式図である。

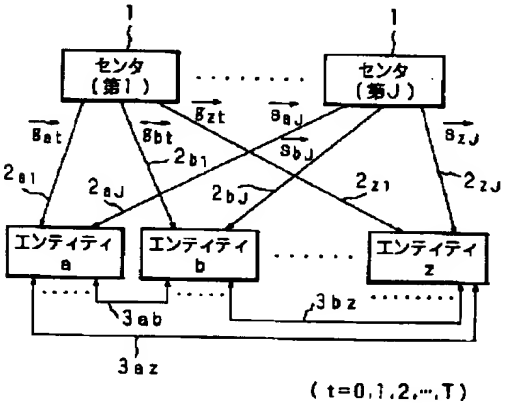
【図３】２人のエンティティ間における情報の通信状態を示す模式図である。

【図４】記録媒体の実施の形態の構成を示す図である。

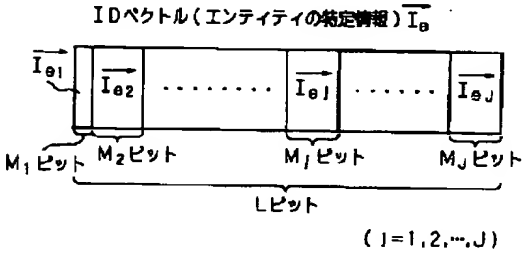
【符号の説明】

１　センタ
１ａ　秘密鍵生成器
１０，２０　メモリ
１１，２１　成分選出器
１２，２２　共通鍵生成器
１３　暗号化器
２３　復号器
３０　通信路
４０　コンピュータ
４１，４２，４３　記録媒体

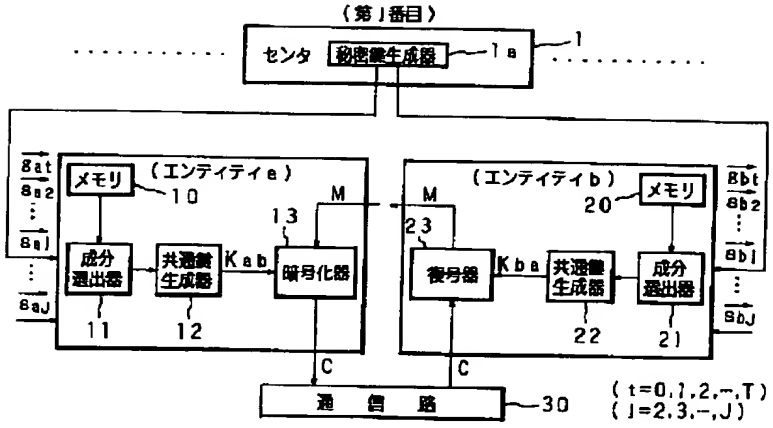
【図１】



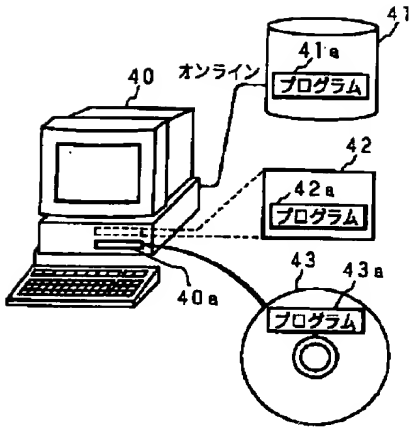
【図２】



【図３】



【図４】



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
		Ｈ０４Ｌ　9/00	６７３Ａ

(72)発明者　村上　恭通
京都府京都市伏見区竹田向代町136番地
村田機械株式会社本社工場内

(72)発明者　辻井　重男
東京都渋谷区神宮前四丁目２番19号

Ｆターム(参考)　5J104 AA16 EA13 EA26 JA03 NA05
PA07